## REMARKS

Claims 2, 11-13, 54-81 and 83-86 are pending in this application. Claim 86 is newly presented. Claims 2, 11-13 and 54-85 have been rejected. Claims 69 and 82 have been cancelled and claims 54, 56, 71, 73 and 84 have been amended. Claims 54, 71, 84 and 86 are independent.

New claim 86 is a method counterpart to pending claim 54. Claim 86 does not present any new matter.

**The Rejection Under**
**35 U.S.C. § 102**

Claims 54-57, 59, 68, 69, 71-74, 82, 84 and 85 have been rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent No. 5,883,810 to Franklin et al. Applicant respectfully traverses this rejection, and submits the following arguments in support thereof.

First, it will be appreciated that the cancellation of claims 69 and 82 renders moot the corresponding portions of this rejection.

Applicant's invention, as recited in claim 54, is directed to an electronic settlement system for effecting a transaction through a communication network. The system has a paying terminal for purchasing an item by a user thereof, the paying terminal including an input unit for inputting authentication information of the user and connecting to the communication network, a billing terminal for charging the user of the paying terminal a purchase amount, the billing terminal being connected to the communication network, a database for storing authentication information of the user and plural authentication methods, and a mediating server performs the settlement of the transaction by mediating a communication between the paying terminal and the billing terminal one-to-one when receiving a transaction ID information from one of the paying terminal and the billing terminal so as to determine that the

paying terminal and the billing terminal are participating in a same purchase, the mediating server setting at least one of the authentication methods selected by either one of the user of the paying terminal and a clerk of the billing terminal in accordance with a content of the transaction. The selected authentication method is processed between the paying terminal and the billing terminal that have been determined to be participating in the same purchase, and one of the mediating server and the billing terminal authenticates the user by using the authentication information stored in the database.

Claim 71 concerns a transaction apparatus for effecting a transaction through a communication network with a paying terminal including an input unit for inputting authentication information of a user and a billing terminal for charging the user a purchase amount. This transaction apparatus has a first communication unit connected to the billing terminal via a first communication network, a second communication unit connected to the paying terminal via a second communication network, a database for storing the authentication information of the user and plural authentication methods, and a processing unit for performing settlement of the transaction by mediating a communication between the paying terminal and the billing terminal one-to-one when one of the first and second communication units receives a transaction ID information from one of the billing and paying terminals so as to determine that the billing and paying terminals are participating in a same purchase. The processing unit processes at least one of the authentication of the user or mediates the authentication of the user selected by either one of the user of the paying terminal and a clerk of the billing terminal in accordance with a content of the transaction, the selected authentication method being processed by the paying and billing terminals, by using the authentication information stored in the database.

According to claim 84 this invention also is directed to a recording medium which stores a program for a computer, communicating with a billing terminal performing billing of a transaction and with a paying terminal performing paying of the transaction, and performs a settlement of the transaction. Such a program includes a first communication module which prompts one to communicate to the billing terminal via a first communication network, a second communication module connected to the paying terminal via a second communication network, a storage module for storing authentication information of a user and plural authentication methods, and a processing module which performs the settlement of the transaction by mediating a communication between the paying and billing terminals one-to-one when one of the first and second communication units receives a transaction ID information from one of the billing and paying terminals so as to determine that the billing and paying terminals are participating in a same purchase. The processing module processes an authentication of the user or mediates the authentication of the user processed by the paying and billing terminals, by using the authentication information stored in the storage module in a manner selected by either one of the user of the paying terminal and a clerk of the billing terminal in accordance with a content of the transaction.

Applicant respectfully submits that the claim features providing for a database for storing authentication information of the user and plural authentication methods and the mediating sever setting at least one of the authentication methods demanded by either one of the user of the paying terminal and a clerk of the billing terminal in accordance with a content of the transaction patentably distinguish over Franklin.

In this regard, it will be understood that, conventionally, a user wishing to use electric money has to obey a predetermined authentication method of the transaction system, for

example, a password authentication method. One of the problems with this inflexible traditional system is that the user and the clerk always have to obey such rules, even in the event that one or both of them believe that the authentication method being used is either too strict or not strict enough for the particular transaction that is being conducted.

For example, if the amount of the purchase in question is just one dollar, requiring the user (buyer) to input their password makes very little sense to the buyer, since the small amount of the transaction means little is at risk and the buyer may not deem the inconvenience of the authentication to be justified. In contrast, the clerk/seller may think that the inconvenience of authentication is justified even though the amount of the transaction is small. In still another situation, a clerk/seller may not require any authentication at all if the user/purchaser is an acquaintance of the clerk/seller, even where the amount of the transaction is relatively large (since the buyer is known to the seller, the seller is effectively vouching for the reliability of the buyer). So the authentication method that the clerk wishes to use can be varied according to the identity of the purchaser/user.

Consequently, in Applicant's claimed invention, the user and the clerk can select their preferred authentication method(s) freely, for example, in accordance with the content of the transaction.

By way of non-limiting example, such aspects of the present invention will be particularly clear in view of the disclosure at, for example, page 29, lines 18-21, page 42, line 21, through page 43, line 29, page 78, lines 12-21, and page 80, lines 1-18, of the specification.

These aspects of the present invention are not taught or even suggested by Franklin. The Office Action effectively **admits** this difference, in view of the Office Action's

observation at page 8, § 12, that "Franklin does not specifically disclose specification of authentication methods based on price."

Although the Office Action contends that Franklin, at col. 7, lines 6-38, teaches setting an agreeable method in accordance with the authentication method stored in the paying terminal database and the authentication method stored in the billing terminal database, that is not an accurate characterization of Franklin. The Office Action mischaracterizes Franklin because Franklin here only teaches a single authentication method, the known use of a public/private key system:

> The customer receives a PIN mailer three to ten days following application submittal. Upon receiving the PIN, the customer invokes the registration module 56 and prepares a "request for a certificate" from the issuing bank. As part of creating the request for certificate, the customer is asked to enter a public key (or one can be provided automatically by the customer computer). The registration wizard 56 generates an associated private key using its own resources, or by calling a cryptographic services library resident on the customer computer. The cryptographic services perform such tasks as encryption, decryption, digital signing, authentication, and hash computations.
>
> **The pair of public and private keys is unique to the customer. The public/private keys form the foundation of public cryptography systems and are based upon a mathematical relationship in which one key cannot be calculated (at least in any reasonable amount of time) from the other key. The holder distributes the public key to other parties and maintains the private key in confidence. Public key cryptography is well known. An example of an asymmetric cipher is the well-known RSA cryptographic algorithm named for the creators Rivest, Shamir, and Adleman.**
>
> The customer computer 28 submits the certificate request to the issuing bank (flow arrow 4 in FIG. 2). The certificate request contains the public/private key pair and the temporary PIN, which serves as a baseline authentication of the customer requesting the certificate.
>
> If the bank still desires to grant an online commerce card to the customer, the account manager 60 at the issuing bank converts the temporary customer account record to a permanent account record in the database 64.

> The bank's account manager 60 assigns a permanent customer account number to the customer account record.

Franklin, at col. 7, lines 6-38 (emphasis added).

Franklin, in its discussion of how a customer makes a purchases, only teaches the use of a single, inflexible security system:

> Upon clicking the button UI 54, a dialog box appears on the display to inform the customer that they have requested a secure card number. The customer is prompted by the dialog box to input a password for identification purposes. This password might be the private key (if the customer knows the key value) or it may be a separate name or number created by the customer. The operating system 48 checks the password prior to allowing access to the certificate store 50. If the password is approved, the transaction module 72 prepares a request for a transaction number, digitally signs the request using the customer's private key, and submits the signed request to the issuing bank's computer 32 via the Internet 34 (flow arrow 2 in FIG. 3). The request contains the certificate originally issued by the bank.

Nowhere is there even a suggestion that the authentication method used can be varied in a particular manner so that one (or several) of a number of different authentication schemes is (are) used. Franklin therefore fails even to suggest at least this aspect of the claimed invention.

It is well-accepted that a reference which fails to identically disclose all the features of an invention cannot anticipate that invention. Here, Franklin fails to even suggest at least those aspects of the invention just discussed, meaning Franklin does not anticipate the present invention.

The remaining rejected claims, claims 55-57, 59, 68, 72-74 and 85, all ultimately depend from and so incorporate by reference all the features of claims 54, 71 or 84, including those features which have just been shown to patentably distinguish over Franklin. These claims

therefore patentably distinguish over Franklin at least for the same reasons as their respective base claims.

For all the foregoing reasons, favorable reconsideration and withdrawal of this rejection are respectfully requested.

**The Rejections Under**
**35 U.S.C. § 103**

Claims 58, 60, 67, 70, 76 and 83 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Franklin, as applied in the foregoing rejection under 35 U.S.C. § 102. Applicant respectfully traverses this rejection, and submits the following arguments in support thereof.

The rejected claims all ultimately depend from and so incorporate by reference all the features of claims 54 and 71, including those features which have just been shown to patentably distinguish over Franklin. These claims therefore patentably distinguish over Franklin at least for the same reasons as their respective base claims, which reasons are incorporated by reference herein.

It also should be noted that the recent decision of the Supreme Court in KSR Int'l v. Teleflex, Inc., No. 04-1350, 550 U.S. __ (U.S. April 30, 2007) does not apply here because the issue before the Court in that case was whether the teachings of two references were properly combined. Here, only a single reference has been applied, and so KSR does not control.

This rejection is also traversed insofar as the Office Action, discussing claims 60, 70, 76 and 83, suggests that because different payment schemes involve different authentication schemes, that remedies Franklin's shortcomings. While this may be true, the arrangement suggested in the Office Action is still inflexible because only a single type of authentication is proposed for each type of payment. Following the Office Action's reasoning, all debit card

purchases would be authenticated using a PIN, and all credit card purchases would be authenticated using the card expiration date. The reasoning of the Office Action in fact is also evidence of the nonobviousness of the present invention, and so the Office Action does not and cannot take the position that such a system would suggest the claimed invention, in which flexibility is achieved by having several different authentication schemes which can be selected for use as desired.

For all the foregoing reasons, favorable reconsideration and withdrawal of this rejection are respectfully requested.

Claim 2 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Franklin, and further in view of U.S. Patent No. 6,038,549 to Davis et al. Applicant respectfully traverses this rejection, and submits the following arguments in support thereof.

Claim 2 depends from and so incorporates by reference all the features of claim 54, including those features which have just been shown to patentably distinguish over Franklin. This claim therefore patentably distinguishes over Franklin at least for the same reasons as claim 54, which reasons are incorporated by reference herein.

Davis only is cited as suggesting a messaging system controller. Even assuming *arguendo* that this is correct, it remains that Davis does not have any teachings that remedy the above-noted deficiencies of Franklin with regard to the present invention. So the claimed invention patentably distinguishes over the combination of Franklin and Davis for at least the same reasons it avoids Franklin alone.

More specifically, while Davis does describe a system in which security is a concern and a customer's identity is verified as part of the transaction process (col. 21, lines 24-29), there is no suggestion of the aspects of the claimed invention providing that the

authentication method used can be varied in a particular manner so that one (or several) of a number of different authentication schemes is (are) used, which was just shown to avoid Franklin.

Davis therefore fails to remedy Franklin's shortcomings, meaning the claims patentably distinguish over the combination of these references for the same reasons that they avoid Franklin alone.

Favorable reconsideration and withdrawal of this rejection are respectfully requested.

Claims 11-13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Franklin in view of U.S. Patent No. 6,332,133 to Takayama. Applicant respectfully traverses this rejection, and submits the following arguments in support thereof.

Claims 11-13 all ultimately depend from and so incorporate by reference all the features of claim 71, including those features which have just been shown to patentably distinguish over Franklin. These claims therefore patentably distinguish over Franklin at least for the same reasons as claim 71, which reasons are incorporated by reference herein.

Takayama only is cited as teaching a purchase history. Even assuming *arguendo* that this is correct, the Office Action does not contend Takayama suggests the aspects of claim 71 already shown to avoid Franklin.

Although Takayama teaches in Figs. 16 and 17, and other Figures, and at col. 60, lines 32-49, and col. 61, lines 14-19, that a service data area has personal information and portrait information, there is no suggestion to use such information in the manner of the present invention. Takayama therefore does not remedy Franklin's deficiencies.

Claims 11-13 patentably distinguish over the combination of Franklin and Takayama. Favorable reconsideration and withdrawal of this rejection are respectfully requested.

Claims 61-63, 75, 77 and 78 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Franklin, and further in view of *Electronic Payment Systems* to O'Mahony (it should be noted that only the cover, first two pages, and pages 62-63 of that reference were cited). Applicant respectfully traverses this rejection, and submits the following arguments in support thereof.

Claims 61-63, 75, 77 and 78 all ultimately depend from and so incorporate by reference all the features of claim 54 or 71, including those features which have just been shown to patentably distinguish over Franklin. These claims therefore patentably distinguish over Franklin at least for the same reasons as claims 54 and 71, which reasons are incorporated by reference herein.

O'Mahony only is cited as suggesting stepped authentication based on price. The cited passage of O'Mahony reads, in pertinent part, "Arrangements to perform online verification of transactions, as well as the policy for requiring online verification, is set by the acquirer. This may involve the setting of a *floor limit*, where any transaction exceeding this limit requires an online check as to the card status." (emphasis in original).

All this portion of O'Mahony teaches is the automatic application of a single inflexible verification scheme whenever a transaction exceeds a floor limit value. This is different from, and does not suggest, at least the aspects of the present invention that provide for a database for storing authentication information of the user and plural authentication methods, or that a mediating server sets at least one of those authentication methods that has been selected

by the user of a paying terminal and/or a clerk using the billing terminal. In other words, O'Mahony only teaches a single authentication scheme, whereas in the present invention, multiple authentication schemes are used and the customer and/or clerk can select the scheme to be used. So O'Mahony does not suggest at least these features of the claimed invention, which features, it will be appreciated, also are not suggested by Franklin.

O'Mahony therefore fails to remedy Franklin's shortcomings, and so the claims patentably distinguish over the combination of these references for the same reasons they avoid Franklin alone.

Favorably reconsideration and withdrawal of this rejection are respectfully requested.

Claims 64-66 and 79-81 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Franklin, and further in view of U.S. Patent No. 6,092,202 to Veil et al. Applicant respectfully traverses this rejection, and submits the following arguments in support thereof.

Claims 64-66 and 79-81 all ultimately depend from and so incorporate by reference all the features of claims 54 and 71, including those features which have just been shown to patentably distinguish over Franklin. These claims therefore patentably distinguish over Franklin at least for the same reasons as claims 54 and 71, which reasons are incorporated by reference herein.

Veil only is cited as suggesting biometric authentication. While Veil admittedly discusses biometric data, Veil does not use such data in the manner claimed:

> In one embodiment of the present invention biometric data such as retinal scan, thumbprint, etc. is embedded in the smart card. The smart card holder provides a biometric data sample and enters the PIN. The combination of the biometric data and the PIN precludes repudiation of the electronic transaction because it is a substantially undisputed proof that the smart card holder was authorized to conduct the electronic transactions

> and did conduct the particular electronic transactions. **In this architecture the biometric data therefore is never resident in the nonsecure computing environment**.

(emphasis added).

Because Veil states that the biometric data is kept only in the smart card and "is never resident in the nonsecure computing environment", Veil therefore does not suggest the aspects of the invention as recited in claim 64 providing that the billing terminal (which would be part of what Veil characterizes as the nonsecure computing environment) is a cashier terminal and the input unit of the cashier terminal inputs at least one of the facial portrait, voice, iris image, retina image, and fingerprint image of the user.

In other words, whereas Veil maintains biometric data only on the smart card and specifically states such biometric data is not otherwise resident in the rest of the system, in the present invention, such data is used **within** the system.[1]

In addition, Veil does not have any teachings concerning plural authentication schemes that remedy the above-noted deficiencies of Franklin with regard to the present invention. So the claimed invention also patentably distinguishes over the combination of Franklin and Veil for at least the same reasons it avoids Franklin alone.

For all the foregoing reasons, favorable reconsideration and withdrawal of this rejection are respectfully requested.

## CONCLUSION

Other than the extension fee authorized in the accompanying Petition For Extension of Time submitted herewith, no fees are believed to be due in connection with the

[1] It will be appreciated that Veil uses the term "nonsecure computing environment" in a very specific manner, and that Applicant's characterization of the present invention is not meant to suggest Applicant's system is in any way insecure. Rather, applicant's system operates in a very different way than Veil, and so it achieves security in a different manner.

filing of this paper. Nevertheless, should the Commissioner now or hereafter deem any fees to be now or hereafter due, the Commissioner is authorized to charge any and all such fees to Deposit Account No. 19-4709.

Favorable consideration and prompt allowance of this application is respectfully requested. In the event that there are any questions, or should additional information be required, please contact Applicant's attorney at the number listed below.

Respectfully submitted,

*/David L. Schaeffer/*

David L. Schaeffer
Registration No. 32,716
Attorney for Applicant
STROOCK & STROOCK & LAVAN LLP
180 Maiden Lane
New York, New York 10038-4982
(212) 806-6677